

MAANPUOLUSTUSKORKEAKOULU

**INFORMAATIOSODANKÄYNNIN TUOMAT HAASTEET
ILMAVOIMIEN PÄÄJÄRJESTELMIIN**

Kandidaatintutkielma

Kadetti

Paulus Kärnä

Kadettikurssi 96

Ilmavoimien ohjaajalinja

Huhtikuu 2012

MAANPUOLUSTUSKORKEAKOULU

Kurssi Kadettikurssi 96	Linja Ilmavoimien ohjaajalinja
Tekijä Kadetti Paulus Kärnä	
Tutkielman nimi Informaatioidankäynnin tuomat haasteet Ilmavoimien pääjärjestelmiin	
Oppiaine, johon työ liittyy Taktiikka	Säilytyspaikka Maanpuolustuskorkeakoulun kurssikirjasto
Aika Huhtikuu 2012	Tekstisivuja 23 Liitesivuja 0
TIIVISTELMÄ <p>Informaatioidankäynti on sodankäynnin osa-alue, jonka tutkimus- ja kehittämistyö alkoi laajamittaisesti 1990-luvun Yhdysvalloista. Suomen kaltaisissa voimakkaasti kehittyvissä tietoyhteiskunnissa informaatioidankäynti luo erilaisia haasteita, joihin vastaaminen on välttämätöntä tehokkaan puolustuksen takaamiseksi. Tutkielmassa tarkastellaan informaatioidankäynnin tuomia haasteita Ilmavoimien pääjärjestelmiin, joita ovat johtamis- ja taistelujärjestelmä, tukeutumisjärjestelmä ja valvontajärjestelmä.</p> <p>Tutkielman pääkysymys on: Mitä haasteita informaatioidankäynti aiheuttaa Ilmavoimien pääjärjestelmien toiminnalle?</p> <p>Tutkielman alakysymyksiä ovat:</p> <ul style="list-style-type: none">– mitä on informaatioidankäynti ja mitkä ovat sen lajit?– miten informaatioidankäynti vaikuttaa Ilmavoimien johtamisjärjestelmän näkökulmasta tarkasteltuna?– mitä on informaatioidankäynti tarkasteltuna Ilmavoimien muiden pääjärjestelmien näkökulmasta? <p>Tutkielma jakautuu kahteen tärkeimpään osaan. Ensimmäisessä käsitellään informaatioidankäyntiä ja ilmavoimien pääjärjestelmiä käsitteellisellä tasolla sekä kerrotaan informaatioidankäynnin tutkimuksesta ja historiasta. Toisessa osassa informaatioidankäynti sidotaan Ilmavoimien toimintaan. Siinä tarkastellaan haasteita, joita informaatioidankäynti luo Ilmavoimien järjestelmille.</p> <p>Tutkielma on luonteeltaan laadullinen ja lähestymistapana aiheeseen käytetään aineistopohjaista teoriaa. Tutkielmassa käytetään myös aineistoanalyysin ja teemoittelun keinoja. Tärkein käytettävä lähde on Martin C. Libickin vuoden 1995 kirjoittama kirja ”What Is Information Warfare?”, jonka avulla tutkimuskohdetta määritellään. Lisäksi tutkimuksen aineistoon kuuluvat aiheesta kirjoitettu muu kirjallisuus, lehtiartikkelit, tutkimustyöt ja internetlähteet.</p> <p>Tutkielman mukaan informaatioidankäynti luo Ilmavoimien pääjärjestelmille lukuisia haasteita, jotka liittyvät muun muassa informaatioteknologian kehitykseen, nykyisen sodankäynnin epäsymmetrisyyteen ja kustannustehokkuuteen. Haasteiden tiedostaminen on tärkeää toimivan puolustusjärjestelmän takaamiseksi.</p>	
AVAINSANAT Informaatioidankäynti, informaatio, tieto, ilmavoimat, Ilmavoimien pääjärjestelmät	

INFORMAATIOSODANKÄYNNIN TUOMAT HAASTEET ILMAVOIMIEN PÄÄJÄRJESTELMIIN

SISÄLLYSLUETTELO

1 JOHDANTO	1
2 TUTKIELMAN TEOREETTINEN TAUSTA	3
2.1 Tutkimusmenetelmä.....	3
2.2 Tutkielman viitekehys ja tutkimusongelma	4
2.3 Rajaukset	5
3 INFORMAATIOSODANKÄYNTI JA ILMAVOIMIEN PÄÄJÄRJESTELMÄT	6
3.1 Informaatioidankäynti käsitteenä historiasta nykypäivään.....	6
3.2 Katsaus Ilmavoimien pääjärjestelmien nykytilaan	12
4 INFORMAATIOSODANKÄYNNIN TUOMAT HAASTEET ILMAVOIMIEN PÄÄJÄRJESTELMIIN	15
4.1 Yleisiä informaatioteknologian kehitysnäkymiä.....	15
4.2 Haasteita Ilmavoimien näkökulmasta	15
5 YHTEENVETO	19
6 TUTKIELMAN ARVIOINTI	22
LÄHDELUETTELO	24

vuoden 2007 alussa ja se suorittaa jatkuvasti viranomaisyhteistyön kehittämistä, joka tähtää verkottumisen lisäämiseen sekä kansallisella että kansainvälisellä tasolla.⁴

Yhdysvallat on informaatioidankäynnin johtava tutkija ja kehittäjä⁵. Sen vuoksi amerikkalaista julkista tutkimus- ja kirjallisuustietoa on runsaasti saatavilla. Tutkielman lähdemateriaalin hankintaprosessista todettakoon, että Suomessa aiheeseen liittyvät julkisen tason tutkimukset ovat kuitenkin harvinaisia. Puolustusvoimissa Jukka Jokinen on tehnyt vuonna 2000 esiupseerikurssin tutkimuksen, jonka aiheena on ”Informaatioidankäynnin käsitteellinen kehittyminen 1990-luvulla”.⁶ Lisäksi aihetta sivuten on laadittu muutamia kandidaatti- ja maisteritason tutkielmia, joissa informaatioidankäyntiä tarkastellaan sen yksittäisten osa-alueiden näkökulmasta.⁷

Tämä tutkielma käsittelee informaatioidankäynnin tuomia haasteita Ilmavoimien pääjärjestelmiin. Varsinkin käynnissä olevan järjestelmien muutosprosessin aikana ja sen jälkeen uudistuneen toimintaympäristön vuoksi tulee uskottavan puolustuksen lisäksi pohtia myös uusien järjestelmien mukanaan tuomia sisäisiä haasteita. Tutkimustyön aihe on edellä mainittujen seikkojen vuoksi erittäin ajankohtainen ja sen tarkoitus on lisätä lukijan tietämystä informaatioidankäyntiin liittyvissä asioissa. Lisäksi se antaa eri toimijoille valmiuksia toimia nykyajan ja tulevaisuuden verkostoituneessa järjestelmäympäristössä.

⁴ *Verkostopuolustus*, Puolustusvoimien johtamisjärjestelmäkeskuksen sidosryhmälehti, syksy 2010, s. 9, <http://issuu.com/zeelandsociety/docs/vepu2/6>, 14.11.2011.

⁵ Jokinen, Jukka: *Informaatioidankäynnin käsitteellinen kehittyminen 1990-luvulla*, Esiupseerikurssin tutkielma, Maanpuolustuskorkeakoulu, 2000, s. 3.

⁶ Jokinen (2000).

⁷ Reihe, Sofia: *Disinformaatio informaatioidankäynnin välineenä*, Maanpuolustuskorkeakoulu, 2004, Puranen, Toni: *Fyysinen vaikutus informaatioidankäynnin osana*, Maanpuolustuskorkeakoulu, 2004, Kontoniemi, Jaakko: *Elektronisen sodankäynnin vaikutukset MST-järjestelmään*, Maanpuolustuskorkeakoulu, 2003.

2 TUTKIELMAN TEOREETTINEN TAUSTA

2.1 Tutkimusmenetelmä

Tutkielma on luonteeltaan kvalitatiivinen ja pohdiskeleva. Tutkimusotteeltaan se on aineistopohjainen, jolloin tutkimusasetelma kytkeytyy jo aiemmin saavutettuun teoriapohjaan.⁸ Lähtökohtana on kuitenkin se, että vastaus tutkimusongelmaan ei ole löydettävissä suoraan tietystä lähdemateriaalista. Tutkimuksessa nojaututaan erilaisiin dokumentteihin perustuvaan tietoon ja käytetään hyväksi teemoittelun ja sisällönanalyysin keinoja.

Lähdemateriaaliin perehdyttäessä tutkijan on muistettava lähdekriittisyys. Lähdekritiikki on tutkimusmenetelmä, jonka avulla arvioidaan lähteen käyttökelpoisuutta tutkimuksessa.⁹

Lähdekriittisessä pohdinnassa lähtökohtana on selvittää, mihin tutkittava lähde kulloinkin pyrkii. Esimerkiksi poliittisissa kirjoituksissa asiat esitetään monesti oman näkökulman kannalta suotuisassa valossa. Kirjoitettua dataa tutkittaessa myös kirjoittajan taustat kertovat paljon lähteen käytettävyydestä tutkimuslähteenä. Tutkielmassa on käytetty kirjallisuuteen, aikaisempiin tutkimuksiin, lehtiartikkeleihin, dokumentteihin sekä internetlähteisiin perustuvaa tietoa, josta suurin osa on todennäköisesti tuotettu valikoiden.

Informaatiosodankäyntiä tutkittaessa on huomioitava, että koska sen teorioiden ja sovellusten johtava tutkija ja kehittäjä on Yhdysvallat, myös merkittävä osa tutkimuksen lähdemateriaalista on amerikkalaisten kirjoittajien tuottamaa. Kirjoitetut lähteet pyritään joka tapauksessa varmentamaan eri aineistosta tarkastamalla, jotta lähdetieto on luotettavaa.

Teemoittelu toimii usein tutkimuksissa ensimmäisenä analysointitapana.¹⁰ Siinä pyritään selvittämään tutkimuksen keskeisimpiä teemoja, mikä toteutetaan tutustumalla tarkasti tutkimuksen kannalta olennaiseen aineistoon. Teemoittelussa on tärkeää, että tutkija esittää myös omia johtopäätöksiä eikä ainoastaan esitä havaintoja sitaattien muodossa. Aineistosta pyritään löytämään olennaisia aiheita tutkimusongelman kannalta.¹¹ Analyysi aloitetaan pienistä yksityiskohdista, joiden avulla edetään kohti suuremman kokonaisuuden hallintaa.

⁸ Huttunen, Mika ja Metteri, Jussi (toim.): *Ajatuksia operaatiotaidon ja taktiikan laadullisesta tutkimuksesta*, Maanpuolustuskorkeakoulu, 2008, s. 45. Lähestymistapana aineistopohjainen teoria (engl. Grounded Theory) tarkoittaa sitä, että tutkimuksen teoria muotoillaan tutkittavan aineiston tai teorianmuodostuksen perusteella. Aineistopohjaista teoriaa voidaan pitää yleisenä tapana ajatella ja käsitellä aineistoa.

⁹ Opetushallitus: *Lähde esiin*, http://www03.edu.fi/oppimateriaalit/lahdeesiin/1_2.html, 12.12.2011.

¹⁰ Huttunen ja Metteri (2008), s. 54.

¹¹ Sama, s. 54.

Tutkielman aineiston analyysiä jatketaan sisällönanalyysin keinoin, eli materiaalia pyritään kuvaamaan sanallisesti. Sisällönanalyysissä aineistoa tarkastellaan erittelemällä, yhtäläisyyksiä ja eroja etsimällä sekä tiivistämällä.¹² Analyysi suoritetaan tässä tutkielmassa teorialähtöisesti asettamalla vanhat teoriat tutkimusongelman asettamaan viitekehykseen.

2.2 Tutkielman viitekehys ja tutkimusongelma

Tutkielman viitekehystenä on Ilmavoimien pääjärjestelmien asema osana kaikkien puolustushaarojen suorittamaa operointia suhteessa informaatioidankäynnin luomiin haasteisiin. Aihealueen yläkäsitteenä on informaatioidankäynti ja alakäsitteisiin kuuluvat muun muassa informaatioidankäynnin osa-alueet, joita tutkimuksessa tarkastellaan. Alakäsitteistöä ovat myös Ilmavoimien johtamis-, tukeutumis-, taistelu- ja valvontajärjestelmät.

Tutkielman pääkysymyksenä on: ”Mitä haasteita informaatioidankäynti aiheuttaa Ilmavoimien pääjärjestelmien toiminnalle?”

Tutkielman alakysymyksiä ovat:

Mitä on informaatioidankäynti ja mitkä ovat sen lajit?

Miten informaatioidankäynti vaikuttaa Ilmavoimien johtamisjärjestelmän näkökulmasta tarkasteltuna?

Mitä on informaatioidankäynti tarkasteltuna Ilmavoimien muiden pääjärjestelmien näkökulmasta?

Tutkielman tavoitteena on selventää sekä tutkijalle että lukijalle informaatioidankäynnin osa-alueita käsitteistön osalta ja herättää kysymyksiä, ajatuksia ja pohdintoja ajatellen informaatioidankäynnin tuomia haasteita Ilmavoimien pääjärjestelmien toiminnalle. Jokainen Ilmavoimien työntekijä on jollain tavalla sidoksissa kyseisiin järjestelmiin ja tietämys asioista edistää henkilöstön ammattitaitoa olennaisesti.

¹² Huttunen ja Metteri (2008), s. 55.

2.3 Rajaukset

Tutkielman laajan aihealueen ja julkisen luonteen vuoksi selkeä ja tiukka rajaus nousee huomattavan suureen arvoon. Tutkielmassa käsitellään suurimmalla painoarvolla Ilmavoimien johtamisjärjestelmää. Näin ollen Ilmavoimien taistelu-, valvonta- ja tukeutumisyjärjestelmät jäävät vähemmälle huomiolle. Tutkielman painopiste keskittyy Ilmavoimien järjestelmien osalta informaatiotodankäynnin näkökulmasta keskeisimpiin aihepiireihin.

Koska kyseessä on taktiikan tutkielma, siinä esiintyvien järjestelmien tekninen esittely on jätetty vähäiseksi ja vastaavasti käytössä olevien resurssien tehokkaaseen käyttöön tähtäävä pohdinta on etusijalla. Tutkielmassa ei myöskään paneuduta spesifisti jonkin toimijan tai osapuolen informaatiotodankäyntiin liittyvään kapasiteettiin vaan tarkastellaan esimerkiksi erilaisia vaikuttamisen keinoja yleisellä tasolla puolueettomasta näkökulmasta. Tutkielmassa kuitenkin pyritään huomioimaan Puolustusvoimien puolustuksellinen toimintamalli, jonka vuoksi osa informaatiotodankäynnin vaikutuskeinoista jää selvästi vähemmälle huomiolle. Tarkoituksena on tarkastella informaatiotodankäynnin aiheuttamia haasteita, ei niinkään antaa yksiselitteisiä ratkaisuja esille nouseviin ongelmiin.

3 INFORMAATIOSODANKÄYNTI JA ILMAVOIMIEN PÄÄJÄRJESTELMÄT

3.1 Informaatiosodankäynti käsitteenä historiasta nykypäivään

Informaatiosodankäynti käsitteenä esiintyi tiettävästi ensimmäistä kertaa vuonna 1976 Thomas P. Ronan Boeing-yhtiölle tekemässä tutkimuksessa ”Weapon Systems and Information War”¹³, jossa esitetään varhaisimpia ideoita informaatiosodankäynnin saralla. Ronan tutkimukseen on viitattu usein myös myöhemmissä aiheeseen liittyvissä kirjoituksissa. Rona totesi aikanaan hyvin laajasti, että informaatiosodankäynti tarkoittaa osapuolten pyrkimystä saavuttaa tavoitteitaan informatiivisin keinoin, ja informaatiota voidaan käyttää sekä puolustuksellisessa että hyökkäyksellisessä tarkoituksessa.¹⁴ Teoriat ovat luonnollisesti muuttuneet ja tarkentuneet lähestyttäessä nykypäivää erityisesti sen vuoksi, että informaatioteknologian vallankumous alkoi suuressa laajuudessaan vasta 1990-luvulla. Peruseriaatteiltaan Ronan teoria on kuitenkin edelleen täysin paikkansapitävä.

Eversti John Boydin kehittämä OODA-Loop -teoria (Observe, Orient, Decide, Act) vaikutti merkittävästi ajatteluun informaatiosodankäynnistä. Hän julkaisi ideansa ensimmäistä kertaa vuonna 1976 ja päivitti teoriaansa vuoteen 1995 saakka.¹⁵ Boydin alkuperäinen idea pyrki selittämään Yhdysvaltain lentäjien ylivoimaa ilmataisteluissa Korean sodan aikana.

Boydin mukaan päätöksenteko on rationaalisen ajattelun tulos, joka perustuu neljän toiminnon sarjaan (kuva 1). Ensimmäiseksi yksilö havainnoi keräten tietoa ympäristönsä tapahtumista (Observe). Havaintojensa perusteella yksilö muodostaa itselleen käsityksen siitä, millaisia päätöksiä ympäristön tapahtumat häneltä vaativat (Orient). Tämän jälkeen hän tekee päätöksen (Decide) ja toimeenpanee sen (Act).¹⁶ Tavoitteena on pyrkiä saavuttamaan pienempi päätöksenteon kehä kuin vihollisella, jolloin omien toimenpiteiden tuottama vaikutus saadaan aikaan tehokkaammin. Käytännössä se tarkoittaa nopeampia, mutta samalla laadukkaita päätöksiä ja toimia. Ajattelu- ja toimintaketju muodostavat jatkumon, jossa edeltävät ratkaisut vaikuttavat seuraavien toimintojen suorittamiseen, kuten kuvassa 1 on esitetty. Informaatiosodankäynnin keinoin ei ole ainoastaan mahdollista parantaa ja nopeuttaa

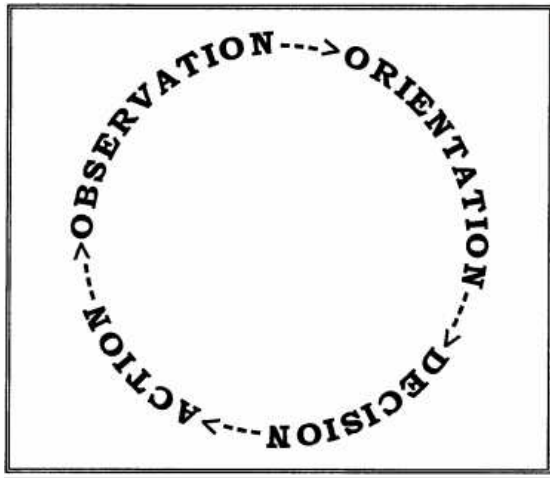
¹³ Leskinen, Aleks: *Informaatiosodankäynti, operaatioturvallisuus ja Puolustusvoimien turvallisuustoiminta*, Pro gradu -tutkielma, Johtamisen laitos, 2006, s. 26.

¹⁴ Libicki, Martin C.: *What is Information Warfare?* National Defence University, 1995, s. 4.

¹⁵ Leskinen (2006), s. 27 - 28.

¹⁶ Schechtman, Gregory M.: *Manipulating the Ooda Loop: The overlooked role of information resource management in Information Warfare*, Air Force Institute of Technology, 1996, s. 34-35.

omaa toimintaa, vaan myös vaikeuttaa vihollisen toimintaa esimerkiksi vihollisen tiedonsaannin estämisen tai tiedon muuntelemisen avulla.¹⁷



Kuva 1: Boydin OODA-loop¹⁸

Informaationsodankäyntiä tutkittaessa toinen merkittävä teoreetikko on Yhdysvaltain ilmavoimista eläkkeelle siirtynyt eversti John Warden, jonka kehittämä teoria kuvaa yksinkertaistetusti vihollisen järjestelmää (kuva 2). Hän esitti, että vihollisen järjestelmä koostuu viidestä eri tasosta, joita ovat¹⁹:

- Johtaminen (Leadership)
- Tuotanto (System Essentials)
- Infrastrukturi (Infrastructure)
- Populaatio (Population)
- Asevoimat (Fielded Military)

Wardenin teorialla oli voimakas vaikutus esimerkiksi Yhdysvaltain käymään 1990-luvun alun Persianlahden sotaan, jota pidetään ensimmäisenä informaationsodankäynnin keinoja hyödyntäneenä sotana.²⁰ Wardenin ideat täsmäaseiden, häivetekniikan, samanaikaisten hyökkäysten ja muiden ilmasodan komponenttien käytöstä vaikuttivat strategisella tasolla Irakin hallitukseen erityisesti informaation siirtymisen osalta.²¹

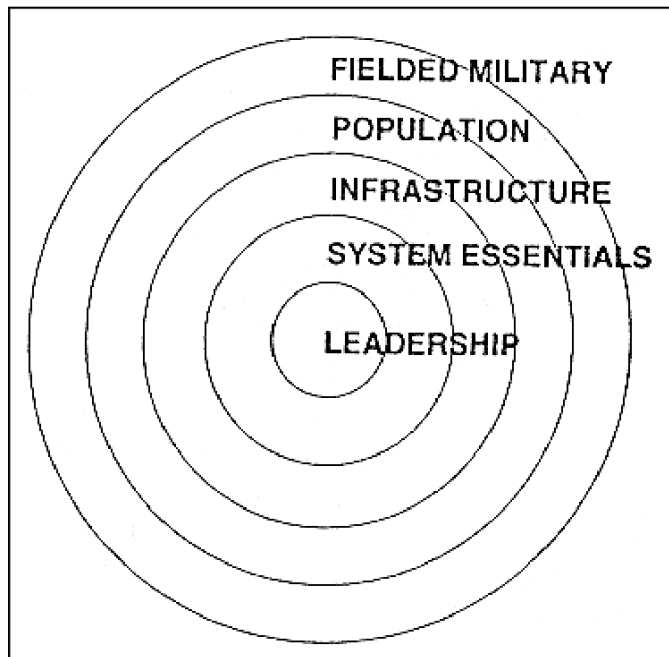
¹⁷ Schechtman (1996), s. 41.

¹⁸ Sama, s. 34

¹⁹ Warden, John A. III: The Enemy as a System, *Airpower Journal*, 1995, s. 5.

²⁰ Leskinen (2006), s. 29.

²¹ Bartholomees, J. Boone (toim.): *USAWC Guide To National Security Issues, Vol I: Theory Of War And Strategy*, Department of National Security and Strategy, 2008, s. 305.



Kuva 2: Vaikuttamisen kehät Wardenin mukaan²²

Suomalaisittain tarkasteltuna informaati sodankäynnillä tarkoitetaan valtion yhteiskunnalliseen tai sotilaalliseen päätöksentekoon sekä kansalaisten mielipiteisiin vaikuttamista informaatioympäristöä hyväksikäyttämällä. Informaati sodankäyntiä voidaan harjoittaa kaikilla sodankäynnin tasoilla yhteiskunnallisin, poliittisin, sosiaalisin, taloudellisin, psykologisin, sotilaallisoin tai viestinnällisin keinoin.²³ Nykykäsityksen mukaan sodankäynti on aina myös informaati sodankäyntiä, joka tähtää informaatioylioivoimaan ja jonka tärkeimpänä tavoitteena on vaikuttaa keskeisimpien kohdeyleisöjen mielipiteisiin.²⁴ Lisäksi informaati sodankäynnillä voidaan lisätä sodan kitkaa, jota syntyy ainoastaan todellisessa sodassa ja jota ei tarkoissakaan suunnitelmissa voida ennakoida tai mallintaa.²⁵ Kitkaa voivat olla aiheuttamassa esimerkiksi informaati sodankäynnin vaikutuksesta syntyneet ongelmat tiedon siirtymisessä eri toimijoiden välillä.

Martin C. Libickin määritelmän mukaan informaati sodankäynnin osa-alueita ovat²⁶:

- Johtamissodankäynti
- Elektroninen sodankäynti
- Psykologinen sodankäynti
- Tiedustelusodankäynti
- Hakkerisodankäynti

²² Leskinen (2006), s. 31.

²³ Suomen turvallisuus- ja puolustuspolitiikka 2004: *Valtioneuvoston selonteko VNS 6/2004*, s. 156.

²⁴ Tienari, Janne ja Meriläinen, Susan: *Johtaminen ja organisointi globaalissa taloudessa*, WSOYpro Oy, 2009, s. 30.

²⁵ Clausewitz, Carl von: *Sodankäynnistä*, Art House, 4. painos, 2005, s. 61.

²⁶ Libicki (1995), s. 7.

- Taloustietosodankäynti
- Kybersodankäynti

Libickin teorian mukaan johtamissodankäynnissä tavoitteen saavuttamiseksi on olemassa kaksi eri lähestymistapaa. Ensimmäinen tapa on lamauttaa vihollinen ”iskemällä vihollisen pää irti ruumiista”.²⁷ Tämä voidaan suorittaa tuhoamalla vihollisen sotilasjohto, jolloin taistelevat osat jäävät irrallisiksi yksiköiksi ja menettävät kykynsä operoida yhtenäisesti ja tehokkaasti. Toinen keino lamaannuttaa vihollinen on katkaista johtoyhteydet, jotka nykypäivänä suurelta osin toteutetaan elektronisin yhteyksin.²⁸ Johtamissodankäynnin tärkeyttä korostaa Yhdysvaltain ilmavoimien everstiluutnantti Norman B. Hutcherson, joka teoksessaan uskoo monikansallisen liittouman menestyksen taustalla Persianlahden sodassa olleen juuri oikealla tavalla ja reaaliaikaisesti suoritettujen johtamissodankäynnin elementit.²⁹

Armeijan sovelluksena elektroninen sodankäynti tarkoittaa kaikkia elektromagneettista säteilyä lähettävien tai käyttävien järjestelmien operointia tai niihin vaikuttamista.³⁰ Elektronisella sodankäynnillä on kolme tavoitetta. Ensimmäinen tavoite on tiedon hankkiminen sähkömagneettisen spektrin kautta passiivisin menetelmin vastustajan joukoista ja järjestelmistä hyvän tilannekuvan ja -tietoisuuden saavuttamiseksi sekä maalien paikantamiseksi. Toinen tavoite on vastustajan tiedustelun, valvonnan, johtamisen ja ase- sekä omasuojajärjestelmien käytön lamauttaminen ja hidastaminen häiritsemällä tai estämällä sähkömagneettisen spektrin käyttöä, harhauttamalla sensoreita sekä lamauttamalla elektronisia järjestelmiä. Kolmantena tavoitteena on oman sähkömagneettisen spektrin käytön valvonta sekä omien joukkojen suojaaminen estämällä ja harhauttamalla vastustajaa saamasta omiin joukkoihin liittyvää tärkeää tietoa. Käytännössä elektroninen sodankäynti jakautuu elektroniseen tukeen, vaikuttamiseen ja suojautumiseen.³¹

Hyvä esimerkki taistelun dominoinnista elektronisen sodankäynnin avulla on vuonna 1982 käyty Bekaan laakson ilmataistelu, jossa Israel tuhosi arvioiden mukaan 82 Syyrian hävittäjää ilman omia tappioita. Israel onnistui elektronisesti häiritsemään ja osin katkaisemaan syyrialalaisten taistelunjohtajien yhteydenpitoa ilma-aluksiin.³²

²⁷ Libicki (1995), s. 10.

²⁸ Sama, s. 13-14.

²⁹ Hutcherson, Norman B.: *Command & Control Warfare: Putting Another Tool In The War-Fighter's Database*, Air University Press, 1994, s. 4.

³⁰ Spezio, Anthony E.: *Electronic Warfare Systems, IEEE Transactions On Microwave Theory And Techniques, Vol. 50, No. 3, 2002, s. 633.*

³¹ *Ilmatorjuntaupseeri 4/2005*: Jyri Kosola ja Janne Jokinen: Elektroninen sodankäynti - osa 1.

³² Libicki, Martin C.: *Defending Cyberspace And Other Metaphors*, National Defence University, 1997, s. 59.

Psykologisessa sodankäynnissä keskitytään enemmän ihmismieleen kuin erilaisiin teknisiin järjestelmiin vaikuttamiseen.³³ Sen vuoksi se on vanhin informaatio-sodankäynnin osa-alue. Suomalaisen määritelmän mukaan psykologinen ajattelun tukiprosesseihin vaikuttaminen on ihmisten arvostuksiin, asenteisiin, tunteisiin, motiiveihin, päätöksentekoon ja käyttäytymiseen puuttumista.³⁴ Psykologista vaikuttamista voidaan suorittaa esimerkiksi fyysisen tuhoamisen kautta. Eräs psykologisen sodankäynnin sovelluksista on syyskuun 11. päivän terrori-isku Yhdysvalloissa. Iskulla saatiin aikaan laajaa pelkoa ja paniikkia koko Yhdysvaltain kansakunnassa. Psykologinen puolustus taas on poikkeusoloissa käytettävää kansakunnan henkistä kestävyttä, puolustustahtoa ja vastarintahenkeä vahvistava maanpuolustuksen osa-alue.³⁵ Perimmäisenä tarkoituksena psykologisella puolustuksella on puolustus- ja taistelutahdon säilyttäminen sekä vahvistaminen. Voidaan sanoa, että psykologisella sodankäynnillä on kautta historian ollut sekä poliittinen että sotilaallinen ulottuvuus.

Psykologisen sodankäynnin määrittelyä vaikeuttaa sen monimuotoisuus. Yleinen väärinkäsitys on se, että muilla sodankäynnin muodoilla ei olisi psykologisia vaikutuksia vaan ainoastaan fyysisiä seurauksia.³⁶ On kuitenkin muistettava, että sota aiheuttaa aina kaikissa muodoissaan myös joko suunniteltuja tai suunnittelemattomia psykologisia vaikutuksia.

Viime vuosikymmenien voimakas teknologian kehittyminen on antanut kansainvälisille mediatoimijoille mahdollisuuden lähettää TV- ja radiolähetyksiä reaaliaikaisesti myös sotakentiltä.³⁷ Lähetystoimintaa oikein käsittelemällä valtioiden johtoelimet voivat tehokkaasti vaikuttaa haluamallaan tavalla kansan mielipiteisiin. Myös internet on lisännyt eri osapuolten mahdollisuuksia psykologisen sodankäynnin saralla.

Perinteisesti tiedustelutietoa on käytetty oman päätöksenteon raaka-aineena samanaikaisesti pyrkien heikentämään vastustajan päätöksentekijöiden sekä tiedustelun toimintaedellytyksiä.³⁸ Tiedusteluperusteisessa sodankäynnissä (Intelligence-Based Warfare) saavutettua tiedustelutietoa käytetään ennemminkin suoraan asejärjestelmien ohjaamiseen operaatioissa kuin yleiseksi johtamisen perusteiksi. Nykyaikainen sodankäynti on suuntautumassa yhä kasvavassa määrin tietokone- ja automaatioperusteiseksi. Sen vuoksi myös nopean päätöksenteon tärkeys korostuu. Esimerkiksi amerikkalainen JSTAR -tutkakone ja sen

³³ Libicki (1995), s. 35.

³⁴ Berger, Heidi: *Venäjän informaatio-psykologinen sodankäyntitapa terrorismintorjunnassa ja viiden päivän sodassa*, Maanpuolustuskorkeakoulun johtamisen ja sotilaspedagogiikan laitos, 2010, s. 16.

³⁵ Sama, s. 16.

³⁶ Speier, Hans: *Psychological Warfare Reconsidered*, Defence Technical Information Center, 1951, s. 2.

³⁷ Libicki (1995), s. 36.

³⁸ Leskinen (2006), s. 87.

ohjaama ATACMS -tykistöohjusjärjestelmä mahdollistavat tunnin reagointiajan sadan kilometrin säteellä sijaitsevan kohteen havaitsemisesta sen tuhoamiseen.³⁹

Tiedustelusodankäyntiä voidaan tarkastella myös osana Boydin OODA -kehää.

Tiedustelutieto esimerkiksi tuhottavasta kohteesta saavutetaan (Observe) ja prosessoidaan (Orient), minkä jälkeen tehdään päätös kohteen tuhoamisesta (Decide). Kohde tuhoetaan (Act) osittain automaatioon perustuvalla asejärjestelmällä. Myös tässä tapauksessa voidaan todeta, että nopeamman päätöksenteon kehän omaava osapuoli saavuttaa edun.

Hakkerisodankäynti voidaan määritellä vihamieliseksi toiminnaksi erilaisissa tietoverkoissa. Käytännössä hakkerisodankäynnin tavoitteena on tietoverkoissa sijaitsevan informaation hankinta, manipulointi ja tuhoaminen.⁴⁰ Hakkeritoiminta käy nykyaikana jatkuvasti tehokkaammaksi sodankäynnin muodoksi, jonka puolesta puhuu CIA:n entisen johtajan John M. Deutschin lausunto vuodelta 1996. Deutschin mielestä hakkerisodankäynti oli tuolloin toiseksi vakavin uhka Yhdysvaltain turvallisuudelle heti joukkotuhoaseella suoritettavan iskun jälkeen.⁴¹ Kun vielä otetaan huomioon tietoverkkojen räjähdysmäinen kasvu Deutschin ajoista, voidaan puhua erittäin vakavasti otettavasta sodankäynnin muodosta.

Hakkerisodankäynti ei ole välttämättä valtioiden välistä toimintaa. Yleisesti saatavilla olevalla ja toiminnan mahdollistavalla teknologialla periaatteessa kuka tahansa riittävän välineistön ja tietotaidon omaava yksityishenkilö tai ryhmittymä voi aiheuttaa vakavia uhkia valtion turvallisuudelle.

Eräs kuuluisimmista hakkerisodankäynnin sovelluksista on Iranin ydinaseohjelman vuonna 2009 ja seuraavana vuonna valkovenäläisen Natanz -ydinvoimalaitoksen lamauttanut Stuxnet -haittaohjelma. Ohjelman kehittäjä on edelleen arvoitus, mutta hankkeen laajuus huomioon ottaen tekijän on asiantuntijoiden mukaan oltava joko valtio tai useampien valtioiden liittouma.⁴² Ainakin Yhdysvaltoja, Israelia ja Venäjää on epäilty. Haittaohjelman myötä Iranista on tullut nykyaikaisen, mullistuneen sodankäynnin näyttämö, jossa taisteluita käydään kyberavaruudessa.

³⁹ Ahvenainen, Sakari, everstiluutnantti (evp.): *Informaatioodankäynti*, luentomateriaali, 2002, s. 50.

⁴⁰ Sama, s. 54.

⁴¹ Libicki (1997), s. 9.

⁴² Mäenpää, Petri: Ilmestyskirjan mato, *Suomen Kuvalehti* 42/2010.

Taloustietosodankäynti perustuu informaation käyttöön taloudellisessa vaikuttamisessa ja sen sovellutukset voidaan jakaa informaatioosaaroon ja talousimperialismiin.⁴³

Informaatioosaarossa lähtökohtana on ajatus, jonka mukaan informaation ja materiaalin saanti ovat valtiolle yhtä tärkeässä asemassa. Informaatioosaarossa valtion teleyhteydet ulkomaille estetään, jolloin kansainvälisen kaupan käyminen ei ole enää mahdollista.

Informaatioimperialismi taas perustuu ajatukseen, että kaupankäynti on sotaa.⁴⁴ Kehittynein teollisuus on tietointensiivistä, jolloin esimerkiksi eri tieteenalojen tutkimus ja sotilaalliset tilaukset kannattaa hoitaa oman maan yrityksiensä toimesta. Rauhanaikaisessa taloustietosodankäynnissä voidaan hyödyntää myös psykologisen, elektronisen ja hakkerisodankäynnin sovellutuksia.

Kybersodankäynnin taistelukenttänä on kyberavaruus. Se muodostuu tietokoneiden välisistä verkoista, joissa digitaalinen tieto säilötään, siirretään ja muokataan. Sen osa-alueita ovat informaatioterrorismi, semanttinen hyökkäys, simulointisota ja Gibson-hyökkäys.⁴⁵

Hyökkäys- ja puolustusohjelmistojen väliset taistelut tietokoneiden välisissä verkoissa ja tiedonsiirtojärjestelmän tietokoneissa ovat tyypillistä kybersodankäyntiä.⁴⁶

3.2 Katsaus Ilmavoimien pääjärjestelmien nykytilaan

Puolustusvoimien johtamisjärjestelmä on muutosprosessissa, jonka tavoitteena on yhdenmukaistaa eri puolustushaarojen toimintaa ja kehittää verkostopuolustuksen toteuttamista. Pohjoismaat kehittävät jatkuvasti uusia yhteistyöalueita ja -muotoja, joiden avulla maiden puolustusvoimien toiminta tehostuu ja suorituskyky paranee.⁴⁷ Yksi yhteistyön tavoitteista on kustannustehokkuuden parantaminen.

Johtamis- ja taistelujärjestelmän tarkoituksena on luoda edellytykset Ilmavoimien päätehtävän, alueellisen koskemattomuuden ja turvaamisen toteuttamiselle. Ilmavoimien johtamisjärjestelmäosastolla siirryttiin vuoden 2007 alussa Nato-rakenteeseen.⁴⁸ Vanha ilmavoimien johtamisjärjestelmä koostui suuresta määrästä erilaisia järjestelmiä ja verkkoja, joiden ansiosta johtaminen kaikilla tasoilla mahdollistettiin. Järjestelmäuudistuksen myötä Ilmavoimien johtamisjärjestelmä integroidaan Puolustusvoimien yhteiseen eli JOINT -

⁴³ Libicki (1995), s. 67.

⁴⁴ Ahvenainen (2002), s. 55.

⁴⁵ Libicki (1995), s.75.

⁴⁶ Ahvenainen (2002), s. 56.

⁴⁷ *Valtioneuvoston selonteko VNS x/2009*, s. 48.

⁴⁸ *Viestimies 4/2007*, s. 9.

tyyppiseen tiedustelu-, valvonta- ja johtamisjärjestelmään (iTVJ).⁴⁹ ITTH -järjestelmästä siirrytään JADEC2- järjestelmään (Joint Air DEFence Command and Control), jolloin voidaan yhdistää sekä ilmavoimien että ilmatorjunnan johtamisjärjestelmätoiminnot.⁵⁰ Muutoksen seurauksena tilannekuva yhtenäistyy, johtaminen helpottuu ja päätöksentekoprosessi nopeutuu.

Ilmavoimien taktista johtamista ollaan myös kehittämässä. Käytännön toteutuksena parannetaan tiedonsiirron nopeutta ilma-aluksen ja maa-aseman välillä, mikä tarkoittaa siirtymistä vanhan VIIRI -järjestelmän käytöstä uuteen Nato-yhteensopivaan Link 16 - tiedonsiirtojärjestelmään.⁵¹ Link 16 -järjestelmä on käytössä useissa maissa eri hävittäjätyypeissä mukaan lukien esimerkiksi F-15 - ja F-16 -hävittäjät.⁵² Järjestelmän on määrä tulla operatiiviseen käyttöön porrastetusti vuoteen 2015 mennessä ja se mahdollistaa muun muassa paremman viestinnän taistelunjohtajan ja torjuntahävittäjän välillä. Niin ikään tiedonsiirtoon liittyen Ilmavoimat on korvannut vastikään operatiiviset TSTJ -pikapuhelin- ja radionohjausjärjestelmänsä Norjasta hankitulla PUKKO -järjestelmällä, jonka myötä siirrytään radio- ja telekommunikoinnissa IP -verkkojen käyttöön.⁵³ Käytännössä IP -verkon käyttö tarkoittaa sitä, että puhe muutetaan digitaaliseen muotoon ja lähetetään paketteina vastaanottajalle.⁵⁴ Pää- ja varatukikohtien hälytyspuhelinjärjestelmänä toimii tällä hetkellä datapohjainen MAISA (Mission Alert and Information System for Airbases), joka korvasi vuonna 2010 vanhentuneen TELMA -järjestelmän.⁵⁵

Tukeutumisyjärjestelmän tarkoitus on nimensä mukaisesti saattaa huollon ja tukeutumisen keinoin mahdolliseksi ilmapuolustuksen toteuttamisen. Sen kehitystyö oli aktiivisimmillaan 1980–90 -luvuilla, jolloin hankintoja suoritettiin muun muassa viesti-, ajoneuvo-, sähkövoima-, ja lennonvarmistuskaluston osalta.⁵⁶ Kehityksen painopisteessä on ollut kansainvälisen valmiustukikohdan toimintojen rakentaminen. Esimerkiksi tällä keinolla tukeutumisyjärjestelmän taistelukestävyyttä pyritään lisäämään.

⁴⁹ *Viestimies* 4/2007, s. 10.

⁵⁰ *Ilmatorjunta* 4/2010, s. 14, http://www.ilmatorjuntaupseeriyhdistys.fi/4_2010/ITU_0410.pdf, 13.11.2011

⁵¹ Moilanen, Mikko, insinöörikapteeni: Ilmavoimille kansainvälisesti yhteensopiva tiedonsiirtojärjestelmä F-18 - koneiden ja johtokeskusten käyttöön, <http://www.puolustusvoimat.fi/wcm/SU+Puolustusvoimat.fi/Puolustusvoimat.fi/Ilmavoimat/Ajankohtaista/Ilmavoimien+tiedotteet/Ilmavoimille+kv+yhteensopiva+tiedonsiirto>, 15.11.2011.

⁵² Air Land Sea Application Center: *TADIL J*, 2000, s. II-5, <http://www.globalsecurity.org/military/library/policy/army/fm/6-24-8/tadilj.pdf>, 14.11.2011.

⁵³ *Ilmatorjunta* 4/2010, s. 14.

⁵⁴ Järvinen, Petteri: *IT-tietosanakirja*, 2. laitoksen 1. painos, Docendo, 2003, s. 745.

⁵⁵ *Ilmatorjunta* 4/2010, s. 15.

⁵⁶ Sama, s. 15.

Ilmavoimien valvontajärjestelmän tehtävä on luoda kattava tilannetietoisuus, jonka pohjalta ilmavoimien puolustus on mahdollista toteuttaa. Puolustusvoimille asetetun tavoitteen mukaisesti valvontajärjestelmän nykyinen kattavuus on tulevaisuudessa ylläpidettävä ja järjestelmien integraation lisääminen on välttämätöntä. Näin mahdollistetaan myös kauaskantoisen tulenkäytön maalien paikkatiedon reaaliaikainen seuranta.⁵⁷ Vuonna 2004 tehtiin hankintapäätös MRT -järjestelmästä (Multi Radar Tracking) luopumisesta ja sen korvaamista MST -järjestelmällä (Multi Sensor Tracking). MST -järjestelmä eroaa MRT -järjestelmästä siten, että siinä yhtenäistä tilannekuvaa luodaan useiden erityyppisten sensoreiden avulla, kun taas MRT -järjestelmä antaa dataa pelkästään tutkilta saatavien havaintojen perusteella. Muita sensoreita edustaa esimerkiksi aisti-ilmavalvonta. Siirtymävaihe on tällä hetkellä käynnissä ja uusi sensorijärjestelmä mahdollistaa eri sensoreiden saavuttaman tiedon yhdistämisen ja analysoinnin ja sitä kautta yhteisen maali-tilannekuvan luomisen ja ylläpitämisen.⁵⁸ Nykyisten keskivalvontatutkien elinkaari on päättymässä ja nykyaikaisilla järjestelmillä varustetut Ranskasta hankittavat tutkat on määrä ottaa käyttöön asteittain vuoteen 2015 mennessä.⁵⁹ Sen lisäksi Suomen käytössä oleville niin ikään ranskalaisille kaukovalvontatutkille suoritetaan MLU -päivitys (Mid Life Upgrade), jonka ansiosta niiden käyttöaika voidaan jatkaa aina vuoteen 2030 saakka.⁶⁰

Muutokset monikansallisessa teleoperaattorikentässä sekä kasvava kybersodankäynnin uhka muodostivat tarpeen kehittää valtion johdon ja yhteiskunnallisesti tärkeiden viranomaisten sekä muiden toimijoiden käyttöön soveltuvan tietoliikennetarkoituksen.⁶¹ Kehitteillä olevan hallinnon turvallisuusverkon (TUVE) tarkoituksena on parantaa valtion johdon päätöksentekokykyä, tilannekuvan muodostamista ja viranomaisten tiedon vaihtoa. Lisäksi hankkeen tavoitteena on parantaa tiedon eheyden ja kiistämättömyyden edellytyksiä kaikissa turvallisuustilanteissa. TUVE -hankkeen keskeisiin periaatteisiin kuuluu, että kriittiset tietoaineistot ja järjestelmät varastoidaan ja hallitaan Suomessa. Hanke myös edistää osaltaan verkostoitumista ja yhteisten prosessien kehittämistä, koska turvallisuusverkon käyttöönoton myötä siihen liittyvät Ilmavoimien sensori- ja taistelunjohtajärjestelmät sekä operatiivisen ja taktisen johtamisen palvelut. Verkon infrastruktuurin sekä palvelujen tuotanto, ylläpito ja tarjonta tullaan keskittämään valtion omistamalle Suomen Erillisverkot Oy:lle.⁶²

⁵⁷ Valtioneuvoston selonteko VNS x/2009, s. 100.

⁵⁸ Ilmatorjunta 4/2010, s. 14.

⁵⁹ Sama, s. 16.

⁶⁰ Sama, s. 16.

⁶¹ Valtiovarainministeriö: *Hallinnon turvallisuusverkko TUVE*, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20110428Hallin/tuve_esite_6versio2.pdf, 15.11.2011.

⁶² Valtiovarainministeriö: *Periaatepäätös 12.5.2011*, <http://valtioneuvosto.fi/tiedostot/julkinen/periaatepaatokset/2011/TUVE/fi.pdf>, 14.11.2011

4 INFORMAATIOSODANKÄYNNIN TUOMAT HAASTEET ILMAVOIMIEN PÄÄJÄRJESTELMIIN

4.1 Yleisiä informaatioteknologian kehitysnäkymiä

Sodankäynnin vallankumouksen aikaansaamiseen ja informaatioylioivoiman saavuttamiseen tähtäävä ajatus informaatioteknologian kehittamisestä sai alkunsa 1990-luvun Yhdysvalloista, josta se on levinnyt ympäri maailmaa.⁶³ Sen vuoksi informaatioteknologian tutkimukseen ja kehittämiseen on panostettu valtavasti viimeisten kahden vuosikymmenen aikana.

Tarkastelemalla yleisiä kehityslinjoja voidaan pohtia, kuinka kyseiset seikat vaikuttavat myös informaatioteknologian sotilaallisiin sovelluksiin.

Informaatioteknologian määritelmän keskiössä on tieto, jonka hankkimista, varastointia, siirtämistä, luokittamista ja yhdistelemistä informaatioteknologia on.⁶⁴ Tietojenkäsittelyn toimintoja suoritetaan tietokoneella, jonka komponentit tuottavat erilaisia tiedonkäsittelyyn liittyviä toimintoja. Ensimmäiset tietokoneet eivät olleet erityisen käytännöllisiä pienen laskentatehon ja suuren koon vuoksi, mutta nykyaikana monituhattokertainen teho- ja muistikapasiteetti saavutetaan taskuun mahtuvalla kannettavalla laitteella. Prosessoritehon kasvu on mahdollistanut esimerkiksi automaation lisäämisen operoitavissa järjestelmissä. Tallennuskapasiteetin lisääntyessä on prosessoitavissa olevan tiedon määrä kasvanut merkittävästi, minkä ansiosta myös prosessorin avulla suoritettu päätöksenteko on tarkentunut.

4.2 Haasteita Ilmavoimien näkökulmasta

Elektronisten laitteiden koon pienentyminen on mahdollistanut asevoimissa liikkuvien järjestelmien käytön. Esimerkiksi suhteellisen helposti liikuteltavat tutkat ovat erittäin yleisiä ja tulosta elektroniikan pienentyneestä tilantarpeesta. Langattoman tiedonsiirron kehittyessä liikuteltavan tutkan lähettämä tieto saavuttaa vastaanottajan lähes reaaliaikaisesti. Uusi teknologia ja taktiikka muuttavat sodankäyntiä nopeuden, tempon, liikkuvuuden, tilannetietoisuuden ja ulottuvuuden suhteen.⁶⁵

⁶³ Raitasalo, Jyri: *Turvallisuusympäristön muutos ja Suomen puolustus*, Strategian laitos, Julkaisusarja 1, Strategian tutkimuksia No 23, 2008, s. 58.

⁶⁴ *Facta 2001*, WSOY, 1986, s. 584.

⁶⁵ *Valtioneuvoston selonteko VNS x/2009*, s. 11.

Verkostoperusteisen puolustusjärjestelmän toteutus luo haasteita järjestelmien ja tiedon suojaamiselle. Esimerkiksi hallinnon turvallisuusverkon tullessa käyttöön täydellisessä laajuudessaan voidaan sanoa, että kaikki Ilmavoimien tärkeimmät yhteydet liittyvät siihen. Yhteen verkon järjestelmään kohdistettu hyökkäys voi näin ollen lamaannuttaa pahimmassa tapauksessa koko järjestelmien kokonaisuuden.

Jatkuva reaaliaikaisuuden tavoittelu on eräs informaatioidankäynnin tuomista haasteista Ilmavoimien pääjärjestelmille. Haastetta lisää erityisesti se, että nykyaikainen teknologian kehittyminen on nopeaa. Siksi omien järjestelmien päivittäminen ja ylläpitäminen tehokkaina vaativat erityisen tarkkaa suunnittelua ja järkevää toteutusta.

Puolustusvoimien järjestelmien ajantasaistamisen ja yhtenäistämisen lisäksi myös henkilöstön koulutus on olennaisessa roolissa informaatioidankäynnin toimintakentän ymmärtämiseksi. Isona haasteena on kuitenkin se, että teknologian kehitys on jatkunut ja jopa kiihtynyt 2000-luvulla. Sen seurauksena informaatioteknologian mahdollistamista sodankäynnin välineistä ei ole pulaa.⁶⁶ Eräs Puolustusvoimien haasteista on selvittää, kuinka käyttää hyödykseen näin valtavaa määrää informaatioteknologian sovelluksia. Samalla on pidettävä huolta henkilöstön riittävän kattavasta koulutuksesta, jotta ammattitaitoinen ote informaatioidankäynnin osalta Puolustusvoimissa säilytetään.

Tietoa on aina pidetty yhtenä tärkeistä sodan voittamiseen liittyvistä elementeistä. ”Tieto on valtaa” -periaatteesta on kuitenkin nykyaikana luovuttava, koska informaatio leviää verkossa salamannopeasti. Kuka tahansa pääsee siihen nykypäivänä käsiksi internetin yleistymisen ansiosta.⁶⁷ Ulottuvuus onkin yksi keskeisistä asioista informaation käytössä sotimisen keinona.⁶⁸ Tiedon ulottuvuutta voidaan verrata perinteisen armeijan pyrkimykseen ulottaa fyysinen asevaikutuksensa mahdollisimman kauas. Informaatioidankäynnissä eräitä ulottuvuuden keinoja ovat esimerkiksi sosiaaliset mediat ja tv, jotka löytyvät jo vähänkin kehittyneemmiltä alueilta ympäri maapalloa. Myös tiedon prosessointi ja ymmärtäminen tuovat haasteita valtiolle, yhteisöille ja asevoimille. Suomessa tähän haasteeseen on vastattu varsin ansiokkaasti ja Suomen on vuonna 2003 arvioitu olevan kehittynein informaatioyhteiskunta.⁶⁹ On myös huomionarvoista, että tällä hetkellä Puolustusvoimissa keskitytään entistä enemmän verkostokeskeisen puolustuksen kehittämiseen, jonka ansiosta tiedon saavuttaminen, analysointi ja käyttö helpottuvat kaikkien puolustushaarojen osalta.

⁶⁶Siltala, Heikki: Blogiajan sodankäyntiä, *Kylkirauta* 4/2008, Kadettikunta Ry:n jäsenlehti, s. 24.

⁶⁷Sama, s. 25.

⁶⁸Rantapelkonen, Jari: *Information Power vs. Military Power*, Strategian laitos, Julkaisusarja 2, No 36, 2006.

⁶⁹Rantapelkonen (2006).

Kylmän sodan ja neuvostouhan loputtua jäi länsimaisessa sodan kuvassa enemmän tilaa sisällissodille ja muille ei-valtiollisille väkivallan käyttötilanteille.⁷⁰ Tämänkaltaisista toimista alettiin 1990-luvulla käyttää määritelmää epäsymmetrinen sota. Suomessa termiä käytettiin ensi kertaa vuonna 2004, jolloin eduskunta totesi Suomeen todennäköisesti kohdistettavan epäsymmetrisen sodankäynnin muotoja kuten informaatioidankäyntiä ja terrorismia.⁷¹ Epäsymmetrisen sodan uhkan rantautuminen myös Suomeen aiheuttaa totta kai uudenlaisia haasteita Suomen puolustusjärjestelmälle. Näihin uhkiin varauduttaessa tehokas tiedonvaihto viranomastoimijoiden välillä on entistä tärkeämmässä roolissa.⁷² Epäsymmetrinen sota laajentaa sodankäynnin toimintaympäristöä vieden vaikuttamisen keinoja fyysisen toimintaympäristön lisäksi verkkoon ja kyberavaruuteen.

Internetin leviäminen ja kehittyminen on tuonut uusia piirteitä informaatioidankäynnin jokaiselle osa-alueelle. Maailma on siirtymässä yhä enemmän aikakaudelle, jossa laatu korvaa määrää, immateriaalinen fyysistä ja konkreettista sekä tieto materiaa.⁷³ Yksittäinen henkilö voi halutessaan aiheuttaa suuriakin tuhoja hakkeritoiminnan avulla. Uhkakuvien määrä on siis myös Puolustusvoimien näkökulmasta laajentunut valtavasti tietotekniikan kehittymisen myötä.

Koska informaatioidankäynti ei ole ainoastaan sodan ajan toimintaa, on myös Ilmavoimille iso haaste selvittää vaikuttamisen keinoja myös rauhan aikana. Tämä ei ainoastaan kohota omaa valmiutta toimia vaan antaa myös perusteet huomata, mikäli oma järjestelmä on joutunut informaatioidankäynnin vaikuttamisen alaiseksi. Oikein onnistuessaan vaikuttamisen alaiseksi joutunut osapuoli ei välttämättä edes saa tietää siihen kohdistuvasta tiedustelusta, elektronisesta sodankäynnistä tai jostain muusta informaatioidankäynnin osa-alueesta.

⁷⁰ Raitasalo (2008), s. 60 - 61.

⁷¹ Rantapelkonen (2006).

⁷² *Valtioneuvoston selonteko VNx/2009*, s. 86.

⁷³ Ahvenainen (2002), s. 56.

Eräs haaste Ilmavoimille on se, että teknologiapainotteisen puolustusjärjestelmän rakentaminen on suhteellisen kallista. Järjestelmän pitäminen ajantasaisena vaatii leikkauksia muilta osa-alueilta, esimerkiksi Suomessa se tarkoittaa sodanajan vahvuuden pudottamista.⁷⁴ Samanaikainen kehitystyö yhtäällä ja säästötoimet toisaalla edellyttävät tasapainon löytämistä kaikilla osa-alueilla. Oikeanlaisten hankintojen suunnittelu ja järkevä toteutus ovat perusedellytyksiä järjestelmien päivittämissä.

⁷⁴ *Kylkirauta 2/2008*, Kadettikunta Ry:n jäsenlehti, s. 16.

5 YHTEENVETO

Informaatioidankäynti esiintyi ensimmäistä kertaa jostakin nykyisessä muodossaan vuonna 1976 Thomas P. Ronan tutkimuksessa, jossa todettiin informaatioidankäynnin olevan osapuolten keinoja tavoitteidensa saavuttamiseen informaation avulla. Todellinen noste informaatioidankäynnin tutkimiseen ja kehittämiseen käynnistyi Yhdysvalloissa ensimmäisen Persianlahden sodan myötä 1990-luvulla. Yhdysvallat on informaatioidankäynnin johtava kehittäjä ja tutkija. Suomessa aihetta alettiin tutkia tarkemmin 2000-luvun alussa.

Informaatioidankäynnin tutkimista ovat ohjanneet voimakkaasti muun muassa amerikkalaisten sotateoreetikkojen John Boydin ja John Wardenin näkemykset sodankäynnistä. Boydin OODA-Loop -teoria on sovellettavissa erinomaisesti informaatioidankäynnin alalla ja sen mukaan päätöksenteko on rationaalisen ajattelun tulos, joka perustuu neljän toiminnon sarjaan. Toiminnot luovat eräänlaisen jatkumon, jossa aiemmat tapahtumat vaikuttavat seuraavien tehtävien ja toimien suorittamiseen. Tätä toimintojen sarjaa nopeuttamalla työskentelyn laatu säilyttäen on mahdollista saavuttaa etulyöntiasema vihollisen suhteen.

John Wardenin kehämallisissa vihollinen nähdään eräänlaisena systeeminä. Systeemissä on viisi eri osa-alueita: johtaminen, tuotanto, infrastruktuuri, populaatio ja asevoimat. Näihin osa-alueisiin oikealla tavalla vaikuttaminen johtaa menestykseen taistelussa ja sodankäynnissä. Wardenin teoria on käytettävyydeltään hyvin laaja-alainen. Kehämallia voidaan soveltaa kokonaiseen valtioon tai vaikkapa vain yhteen ihmiseen, jonka ”järjestelmä” koostuu viidestä tekijästä.

Suomalaisen määritelmän mukaan informaatioidankäynti on valtion yhteiskunnalliseen tai sotilaalliseen päätöksentekoon sekä kansalaisten mielipiteisiin vaikuttamista informaatioympäristöä hyväksikäyttämällä. Informaatioidankäynti on nykypäivänä kiinteä ja merkittävä osa sodankäyntiä. Se tähtää informaatioyivoiman saavuttamiseen ja sen avulla kohdeyleisöön vaikuttamiseen halutulla tavalla.

Martin C. Libicki on jakanut informaatioidankäynnin seitsemään eri osa-alueeseen, joita voidaan pitää kansainvälisellä tasollakin tunnustettuina. Osa-alueita ovat johtamis-, tiedustelu-, taloustieto-, kyber-, hakkeri-, sekä psykologinen ja elektroninen sodankäynti. On selvää, että muun muassa johtaminen ja tiedustelu ovat elintärkeässä roolissa nykyaikaisessa

sodankäynnissä. Informaatiosodankäynnissä on kuitenkin paljon muitakin ulottuvuuksia. Esimerkiksi kybersodankäynti vaikuttaa olevan nousemassa yhä merkittävämmäksi sodankäynnin muodoksi. Hakkeritoiminnalla taas on saatu aikaan suuriakin vaikutuksia aina valtiollisella tasolla asti. Mainitun kaltaiset sodankäynnin muodot lisäävät taistelukentän epäsymmetrisyyttä.

Ilmavoimien pääjärjestelmät ovat laajamittaisessa päivitys- ja yhdenmukaistamisprosessissa. Prosessin tavoitteena on yhdenmukaistaa eri puolustushaarojen toimintaa ja kehittää verkostopuolustuksen toteuttamista. Ilmavoimien johtamis- ja taistelujärjestelmä kokee merkittävimpiä muutoksia. Se muun muassa integroidaan Puolustusvoimien yhteiseen JOINT-tyyppiseen tiedustelu-, valvonta- ja johtamisjärjestelmään. Myös valvonta- ja tukeutumisyjärjestelmät ovat muutosprosessissa, joka tähtää parempaan reagointikykyyn nykyaikaisia uhkia vastaan. Valvontajärjestelmän osalta muutokset pitävät sisällään tutkahankintoja ja -päivityksiä sekä sensorisovellusten kehittämistä. Tukeutumisyjärjestelmän kehittämisellä luodaan edellytyksiä kansainvälisen tason valmiustukikohdan rakentamiselle.

Informaatioteknologian kehitysnäkymistä yleisellä tasolla voidaan todeta, että kyse on valtavaa, jatkuvaa kasvua kokevasta alasta. Tietokonepohjaisten sovellusten kehitys on voimakasta ja automaatio lisääntyy jatkuvasti. Prosessoriteho lisääntyy, mutta vastaavasti tarvittavien laitteiden koko ja hinta laskevat. Merkittävän tallennustehon omaavat tehokkaat tietokoneet luovat edellytyksiä yhä monimutkaisempien ja tarkempien sovelluksien luomiselle.

Nykyaikaisessa sodankäynnissä eräitä avainsanoja ovat nopeus, tempo, liikkuvuus, tilannetietoisuus ja ulottuvuus. Uudistunut teknologia ja nykypäivän taktiikka muuttavat jatkuvasti sodankäynnin luonnetta ja perusolemusta. Sen vuoksi informaatio- ja kybersodankäynti luo suuria haasteita myös Ilmavoimien toiminnalle. Reaaliaikaisuuden tavoittelu on toiminut yhtenä Ilmavoimien järjestelmä uudistusta ohjanneena tekijänä. Ajan tuomiin muutostarpeisiin vastaaminen on haastavaa, varsinkin kun kyseessä on erittäin nopeasti kasvava sovellusalue.

Sodankäynnin epäsymmetrisyys lisääntyy, mikä aiheuttaa suuria haasteita kaikille Ilmavoimien pääjärjestelmille. Puolustushaarojen yhteisen tilannekuvan ja viranomaisyhteistyön tärkeys korostuvat. Esimerkiksi internet luo edellytykset epäsymmetriselle sodankäynnille. Hakkeritoiminnalla saavutettavat vaikutukset voivat olla mittavia, kun taas riski omille tappioille on varsin pieni. Se onkin eräs sodankäynnin alue, jolla ei-valtiolliset toimijat ovat lisänneet toimintaansa.

Informaatiosodankäynti rauhan aikana on myös eräs haasteista, jotka koskevat Puolustusvoimia kokonaisuudessaan. Esimerkiksi tiedustelutoiminnan harjoittaminen rauhan aikana on hyvin yleistä. Ilmavoimille on iso haaste selvittää vaikuttamisen keinoja myös rauhan aikana. Rauhan aikainen toiminta on tärkeää erityisesti puolustuksellisessa mielessä, jolloin voidaan havaita, mikäli omat järjestelmät ovat joutuneet informaatioodankäynnin vaikutukseen.

Kustannustehokkuus on eräs määräävistä tavoitteista Ilmavoimien toiminnassa. Korkeatasoista teknologiaa hyväksikäyttävä puolustusjärjestelmä on hintava ja sen vuoksi kompromissien etsiminen on välttämätöntä. Suomessa uudet hankinnat ja tehokas kehittyminen tarkoittavat sodanajan vahvuuden heikentämistä. Toimintojen priorisointi sekä säästökohteiden löytäminen vähemmän tärkeistä puolustuksen osa-alueista ovat suuria haasteita Ilmavoimille.

6 TUTKIELMAN ARVIOINTI

Tutkimusongelmana oli tutkielman otsikon mukaisesti ”Informaatioidankäynnin tuomat haasteet Ilmavoimien pääjärjestelmiin”. Vaikka tutkimusongelmaa rajattiin johdantoluvussa, oli rajausten mukaisen linjan saavuttaminen vaikeaa. Esimerkiksi informaatioidankäynnin tuomia haasteita oli vaikea luokitella järkeviksi osakokonaisuuksiksi.

Tutkielman pääkysymys oli:

”Mitä haasteita informaatioidankäynti aiheuttaa Ilmavoimien pääjärjestelmien toiminnalle?”

Tutkielman alakysymyksiä olivat:

Mitä on informaatioidankäynti ja mitkä ovat sen lajit?

Miten informaatioidankäynti vaikuttaa Ilmavoimien johtamisjärjestelmän näkökulmasta tarkasteltuna?

Mitä on informaatioidankäynti tarkasteltuna Ilmavoimien muiden pääjärjestelmien näkökulmasta?

Pääkysymystä mietittäessä etukäteen oli vaikea hahmottaa, millaisia keskeisiä piirteitä oli otettava selkeimmin esille, jotta kysymykseen annettaisiin mahdollisimman selkeä vastaus. Osin vastaus jäi kuitenkin pohdinnaksi erilaisista mahdollisista aspekteista, joilla on mahdollista vaikutusta Ilmavoimien pääjärjestelmien toiminnalle ja operoinnille. Tutkielman tärkeimpänä tuloksena voidaan pitää sen herättämiä uusia kysymyksiä, jotka motivoivat Puolustusvoimien henkilöstöä aktiivisesti kehittämään ammattitaitoaan

Alakysymyksiä asetelussa oli tarkoituksena nimenomaan tarkentaa tutkimusongelman käsittelyä ja kohdistaa tutkijan katse oikeisiin asioihin. Informaatioidankäynnin yleinen määrittely oli jälkeempään ajateltuna tärkeänä osana tutkielmaa luomassa sekä tutkijalle että lukijalle taustatietoa ja antamassa ideoita seikoista, jotka kaipaisivat lisähuomiota. Tutkielman pää- ja alakysymyksiin löydettiin vastaukset tyydyttävällä tasolla. Julkisen tason tutkielmassa ei ole mahdollista pureutua syvällisellä tasolla informaatioidankäynnin tuomiin haasteisiin Suomen näkökulmasta. Sen vuoksi esimerkiksi haasteita käsittelevässä kappaleessa tutkielma joutui keskittymään asioihin yleisellä tasolla.

Tutkimustyön alkuvaiheessa tutkija koki isona haasteena rakentaa taktiikan tutkielma aihealueesta, joka varsin suurelta osin perustuu teknisiin periaatteisiin ja järjestelmiin. Taktiikka on taistelun suunnittelua, valmistelua, toteuttamista ja johtamista,⁷⁵ jossa olennaisina pidettäviä käsitteitä ovat esimerkiksi tilannetietoisuus, vastustajan sekä omien joukkojen toimintatapojen tunteminen sekä joukkojen käytön ja resurssien optimaalinen suunnittelu. Kyseisestä näkökulmasta tarkasteltuna tutkielma antaa tarkastellusta aihealueesta käytännönkin kannalta hyödyllistä informaatiota ja valmentaa sotilasjohtajaa päätöksentekoon informaatiosodankäynnin taistelukentällä. Tutkielma herättää kysymyksiä, joita pohtimalla voidaan saavuttaa parempi valmius toimintaan informaatioteknologian kyllästävässä toimintaympäristössä. Siinä mielessä tutkielma on saavuttanut tavoitteensa.

Tutkielman lähdemateriaalin osalta tutkija yllättyi hieman suomalaisen julkisen tason tutkimuksen vähäisyydestä nimenomaan ilmavoimallisessa kontekstissa. Tutkielmassa käytettiin paljon englanninkielistä lähdemateriaalia, jolloin käännoistyötä helpotettiin saatavilla olevan suomenkielisen lähdemateriaalin avulla varsinkin käsitteistön osalta. Lähdekritiikin osalta tutkielmassa käytettyjä tietoja tarkastettiin useammasta eri lähteestä, jolla varmistettiin tutkielman reliabiliteetti. Vaikka osa tärkeimmistä tutkielmassa käytetyistä lähteistä oli jopa yli 20 vuoden takaisia, informaatiosodankäynnin määrittelyssä ne osoittautuivat täysin luotettavaksi ja paikkansapitäväksi tiedoksi.

Tutkielmassa pureuduttiin informaatiosodankäynnin tuomiin haasteisiin Ilmavoimien pääjärjestelmiin ja tarkoituksellisesti jätettiin kattavien ratkaisujen selvittäminen tutkimusasetelman ulkopuolelle. Jatkotutkimuksen tarve voisi siis olla esimerkiksi paneutumisessa myös erilaisiin vaihtoehtoihin, joissa tarjotaan ratkaisu esille tuotuihin haasteisiin. Mahdollisessa jatkotutkimuksessa vaadittaisiin syvällistä perehtymistä sekä sotatekniikan että informaatioteknologian yleisiin perusteisiin, mutta myös käytössä olevien järjestelmäsovellutusten erityispiirteisiin.

Jatkotutkimusta voitaisiin suorittaa myös esimerkiksi informaatiosodankäynnin osa-alueiden saralla. Kuten tutkielmassa aiemmin mainittiin, kybersodan uhan on todettu kasvaneen Suomen alueella. Esimerkiksi siihen paneutuminen voisi siis olla yksi vaihtoehto jatkotutkimuksessa. Katsaus Maanpuolustuskorkeakoulun tietokantaan antaa viitteitä tutkimusten vähäisyydestä kybersodankäynnin alalla.

⁷⁵ Maanpuolustuskorkeakoulu: *Opinto-opas 2011*, Edita Prima Oy, 2011, s. 30.

LÄHDELUETTELO

Ahvenainen, Sakari, everstiluutnantti (evp.): *Informaaiosodankäynti*, luentomateriaali, 2002.

Air Land Sea Application Center: *TADIL J*, 2000, s. II-5,

<http://www.globalsecurity.org/military/library/policy/army/fm/6-24-8/tadilj.pdf>, 14.11.2011.

Bartholomees, J. Boone (toim.): *USAWC Guide To National Security Issues, Vol I: Theory Of War And Strategy*, Department of National Security and Strategy, 2008.

Berger, Heidi: *Venäjän informaatio-psykologinen sodankäyntitapa terrorismintorjunnassa ja viiden päivän sodassa*, Maanpuolustuskorkeakoulun johtamisen ja sotilaspedagogiikan laitos, 2010.

Clausewitz, Carl von: *Sodankäynnistä*, 4. painos, Art House, 2005.

Cox, Joseph L.: *Information Operations in Operations Enduring Freedom and Iraqi Freedom – What Went Wrong?* School of Advanced Military Studies, 2006.

Facta 2001, WSOY, 1986.

Hutcherson, Norman B.: *Command & Control Warfare: Putting Another Tool In The War-Fighter's Database*, Air University Press, 1994.

Huttunen, Mika ja Metteri, Jussi (toim.): *Ajatuksia operaatiotaidon ja taktiikan laadullisesta tutkimuksesta*, Maanpuolustuskorkeakoulu, 2008.

Ilmatorjunta 4/2010, http://www.ilmatorjuntaupseeriyhdistys.fi/4_2010/ITU_0410.pdf, 13.11.2011.

Jokinen, Jukka: *Informaaiosodankäynnin käsitteellinen kehittyminen 1990-luvulla*, Esiupseerikurssin tutkielma, Maanpuolustuskorkeakoulu, 2000.

Järvinen, Petteri: *IT -tietosanakirja*, 2. laitoksen 1. painos, Docendo, 2003.

Konttoniemi, Jaakko: *Elektronisen sodankäynnin vaikutukset MST-järjestelmään*, Maanpuolustuskorkeakoulu, 2003.

Kosola, Jyri ja Jokinen, Janne: Elektroninen sodankäynti - osa 1, *Ilmatorjuntaupseeri* 4/2005.

Kylkirauta: Kadettikunta Ry:n jäsenlehti, 2/2008.

Kylkirauta: Kadettikunta Ry:n jäsenlehti, 4/2008.

Leskinen, Aleks: *Informaattiosodankäynti, operaatioturvallisuus ja puolustusvoimien turvallisuustoiminta*, Pro gradu -tutkielma, Johtamisen laitos, kesäkuu 2006.

Libicki, Martin C.: *Defending Cyberspace And Other Metaphors*, National Defence University, 1997.

Libicki, Martin C.: *What is Information Warfare?* National Defence University, 1995.

Maanpuolustuskorkeakoulu: *Opinto-opas 2011*, Edita Prima Oy, 2011.

Moilanen, Mikko, insinöörikapteeni: Ilmavoimille kansainvälisesti yhteensopiva tiedonsiirtojärjestelmä F-18 -koneiden ja johtokeskusten käyttöön,
<http://www.puolustusvoimat.fi/wcm/SU+Puolustusvoimat.fi/Puolustusvoimat.fi/Ilmavoimat/Ajankohtaista/Ilmavoimien+tiedotteet/Ilmavoimille+kv+yhteensopiva+tiedonsiirto>, 15.11.2011.

Mäenpää, Petri: Ilmestyskirjan mato, *Suomen Kuvalehti* 42/2010.

Opetushallitus: *Lähde esiin*, http://www03.edu.fi/oppimateriaalit/lahdeesiin/1_2.html, 12.12.2011.

Puranen, Toni: *Fyysinen vaikutus informaattiosodankäynnin osana*, kandidaatintutkielma, Maanpuolustuskorkeakoulu, 2004.

Raitasalo, Jyri: *Turvallisuusympäristön muutos ja Suomen puolustus*, Strategian laitos, Julkaisusarja 1, Strategian tutkimuksia No 23.

Reihe, Sofia: *Disinformaatio informaatioidankäynnin välineenä*, kandidaatintutkielma, Maanpuolustuskorkeakoulu, 2004.

Rantapelkonen, Jari: *Information Power vs. Military Power*, Strategian laitos, Julkaisusarja 2, No 36, 2006.

Spezio, Anthony E.: *Electronic Warfare Systems*, *IEEE Transactions On Microwave Theory And Techniques*, Vol. 50, No. 3, 2002.

Schechtman, Gregory M.: *Manipulating the Ooda Loop: The overlooked role of information resource management in Information Warfare*, Air Force Institute of Technology, 1996.

Speier, Hans: *Psychological Warfare Reconsidered*, Defence Technical Information Center, 1951.

Suomen turvallisuus- ja puolustuspolitiikka 2004: *Valtioneuvoston selonteko VNS 6/2004*.

Suomen turvallisuus- ja puolustuspolitiikka 2009: *Valtioneuvoston selonteko VNS x/2009*.

Tienari, Janne ja Meriläinen, Susan: *Johtaminen ja organisointi globaalissa taloudessa*, WSOYpro Oy, 2009.

Valtiovarainministeriö: *Hallinnon turvallisuusverkko TUVE*, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20110428Hallin/tuve_e_site_6versio2.pdf, 15.11.2011.

Valtiovarainministeriö: *Periaatepäätös 12.5.2011*, <http://valtioneuvosto.fi/tiedostot/julkinen/periaatepaatokset/2011/TUVE/fi.pdf>, 14.11.2011.

Verkostopuolustus, Puolustusvoimien johtamisjärjestelmäkeskuksen sidosryhmälehti, syksy 2010, <http://issuu.com/zeelandsociety/docs/vepu2/6>, 14.11.2011.

Viestimies 4/2007, http://www.viestiupseeriyhdistys.fi/viestimies/vm4_07/IV_Joja_alan_muutos.pdf, 14.11.2011.

Warden, John A. III: *The Enemy As A System*, *Airpower Journal*, 1995.